



NETGEAR[®]

ProSafe 5 AP Wireless Management Software WMS105

User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

May 2010
202-10662-01
v1.0

© 2010 NETGEAR, Inc.© 2010 by NETGEAR, Inc. All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

P/N: Part Number TBD v1.0

Technical Support

When you register your product at <http://www.netgear.com/register>, we can provide you with faster expert technical support and timely notices of product and software upgrades.

NETGEAR, Inc.

350 East Plumeria Drive
San Jose, CA 95134 USA

E-mail: support@netgear.com

Web site: <http://www.netgear.com>

Phone: 1-888-NETGEAR, for US & Canada only. For other countries, see your Support information card.

Trademarks

NETGEAR, the NETGEAR logo, ProSafe, Smart Wizard, and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT, and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date
202-10662-01	v1.0	May 2010

Table of Contents

Chapter 1 Getting Started

Installing the Software	5
Logging In	6
System Settings	6
General Settings	6
Time Settings	7
Syslog Settings	8

Chapter 2 Access Point Discovery

Auto Discovery	9
IP Discovery	10
Discovery Results	11
Adding Access Points	12

Chapter 3 Wireless Configuration

Configuring Centralized RF Management	13
Advanced Wireless Settings	15
Configuring QoS	17
QoS for Managed Access Points	17

Chapter 4 Security Configuration

Security Profiles List	18
Editing a Security Profile	19
Rogue Access Points	20
MAC Authentication	21
Radius Server Settings	23
Configuring Guest Access	24

Chapter 5 Monitoring

Summary	25
Access Point Summary	25
Wireless Stations	26
Access Point Status	26
Access Point Status Details	27
Client Status	28
Monitoring Rogue Access Points	28

Chapter 6 Maintenance

Changing Passwords	30
Reset	31
SNMP	31
Remote Management	32
Upgrading Access Point Firmware	32
Backing up Configuration Settings	34
Restoring Settings from a File	34
Downloading Wireless Management Software Logs	35
Diagnostic Ping Window	35
Using Discovery OUI	36

Appendix A Access Point Compatibility

Access Point Supported Firmware Versions	37
Software Features and Access Point Compatibility	38

Index

Getting Started

1


The ProSafe 5 AP Wireless Management Software is a Wireless Management Software that allows you to manage up to 5 NETGEAR wireless access points on a LAN. You can use the Wireless Management Software to:

- Discover NETGEAR access points on the LAN.
- Optimize wireless access point performance with centralized RF management.
- Streamline security configuration tasks.
- Perform maintenance tasks including remote management and firmware updates for NETGEAR access points on the LAN.

Installing the Software

The Wireless Management System software is on the NETGEAR *Resource CD*.

1. Insert the *Resource CD* and the Install Wizard Welcome screen displays. Click **Next**.
2. Read the software license agreement, select the **Agree** radio button, and then click **Next**.
3. Select the destination for the software, and then click **Next**.
4. Select the Start Menu folder for the software, and then click **Next**.
5. To install the software, click **Install**.

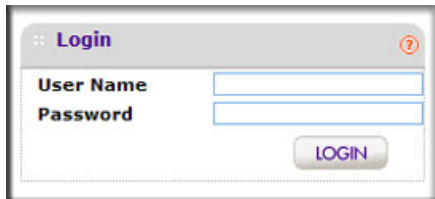
After the software is installed, the  icon appears on the Windows desktop and on the system tray at the bottom of the Windows desktop. You can click this icon to launch the Wireless Management System software.

6. Click **Finish** to exit the wizard.

Logging In

1. To log in to the Wireless Management Software, double-click the application, or right-click it and select Open WMS105 from System tray.

A login prompt displays:



2. If you are logging in for the first time, use the default user name **admin** and password (**password**).

NETGEAR recommends that you change the password to a new, more secure password and record it in a secure location.

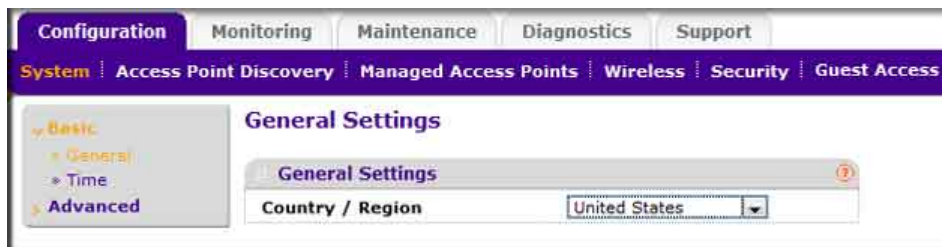
The user interface opens with the Configuration tab selected. This tab is shown in the following section "System Settings."

System Settings

When you log in, the Configuration tab displays General Settings.

General Settings

To navigate to this screen, on the Configuration tab select System > Basic > General:



The General Settings page lets you configure the basic settings of your Wireless Management Software.

- **Name:** This unique value indicates the Wireless Management Software name. By default, the name is wms105.

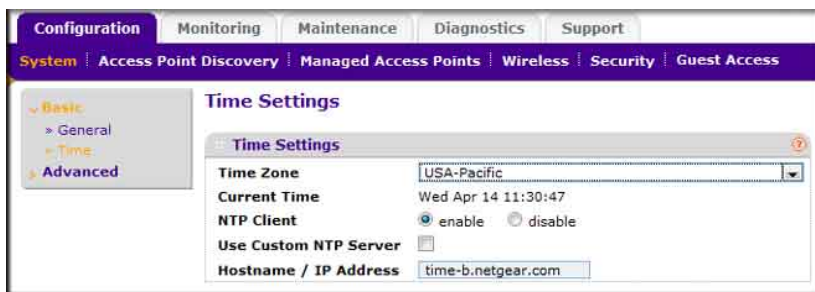
NETGEAR recommends changing the name as soon as possible after setting up. The name must contain only alphabetical characters, numbers, and hyphens, and must be 31 characters or less.

- **Country/Region:** This field displays the region of operation for the Wireless Management Software and the access points managed by the Wireless Management Software. In the United States, the country is preset and cannot be changed on the access points. If the Country/Region is not set up correctly, it could result in the access points being inaccessible by the Wireless Management Software.

For products sold outside the United States, you must select a country or region. It might not be legal to operate the access points in a country/region not shown here. If your location is not listed, check with your local government agency or check the NETGEAR web site for more information on which channels to use.

Time Settings

On the Configuration tab, select System > Basic > Time Settings:

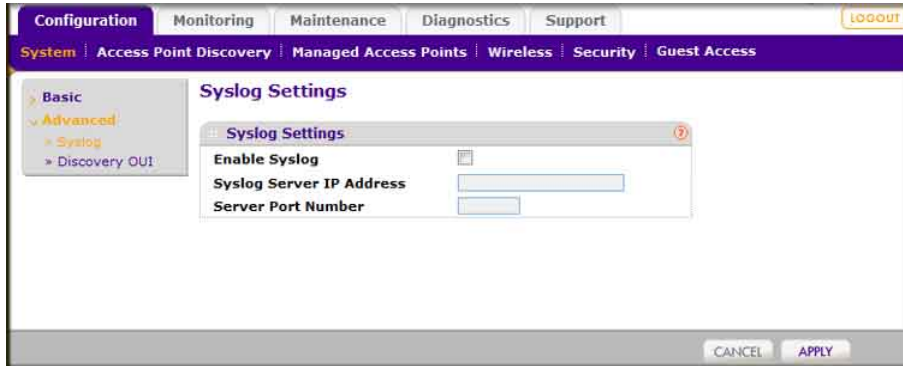


This page lets you configure the time-related settings of your Wireless Management Software and managed access points. It has the following options:

- **Time Zone:** Select the local time zone for your region or country.
- **Current time:** The current time at your location.
- **NTP Client:** Enable this option to use a Network Time Protocol (NTP) server to synchronize the clock of the Wireless Management Software and managed access points. Disable this option if you do not want to use an NTP server.
- **Use Custom NTP Server:** Select this check box if you wish to use an alternate NTP Server. By default, the NETGEAR NTP server is used by the access point.
- **Hostname / IP Address:** Provide the host name or IP address of the NTP server, if you are using a custom NTP server.

Syslog Settings

This page lets you configure the settings to connect to a Syslog server, if you have one configured in your network. Click the Config tab and select System > Advanced.



- **Enable Syslog:** Enable the Syslog settings, if you have a Syslog server on your network.
- **Syslog Server IP Address:** Enter the IP address to which the Wireless Management Software and managed access points send all SysLogs, if the SysLog option is enabled.
- **Server Port Number:** Enter the port number at which your Syslog server is configured to listen to requests. The default port number 514 is filled in when the syslog server is enabled.

Access Point Discovery

2

You can discover supported NETGEAR access points on the LAN that can be managed by the Wireless Management Software. See [Appendix A](#) for a list of compatible access points. The Wireless Management Software supports Auto Discovery and IP Discovery.

- **Auto Discovery:** Use this feature if the Wireless Management Software and all access points on the LAN are in the same IP subnet. This is a Layer 2 discovery method.
- **IP Discovery:** If the Wireless Management Software and access points use different IP subnets, you can use IP discovery to find the access points for each subnet (one subnet at a time). This is a Layer 3 discovery method.

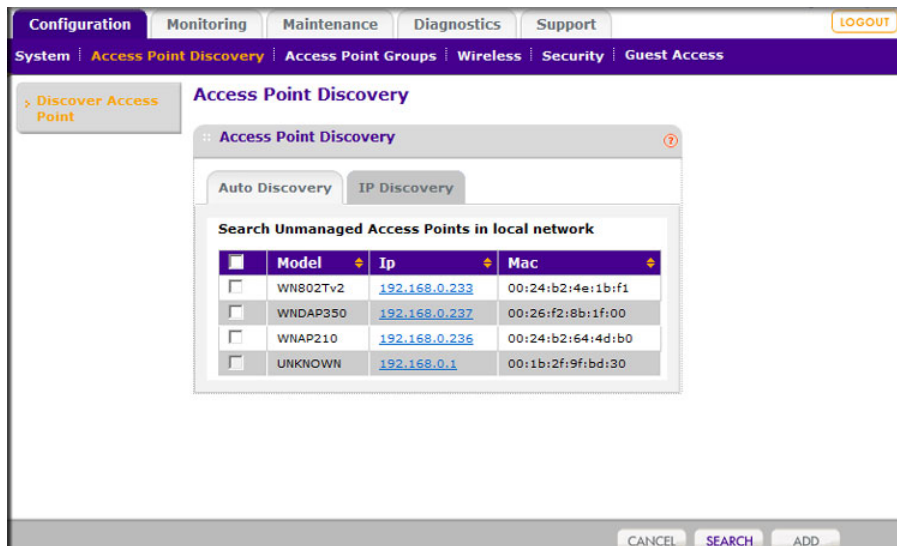
Note: For discovery to work, each access point must have an IP address. If more than one access point has the same default IP address, then only one of them will be discovered with the model number at a time. You will have to add the access point to the managed list, change its IP address and then run discovery again to discover the next access point with the default IP.

Auto Discovery

Use Auto Discovery if the Wireless Management Software and all access points on the LAN are in the same IP subnet. The process of Auto Discovery depends on how your access points are configured.

To use Auto Discovery:

1. On the Configuration tab select Access Point Discovery.



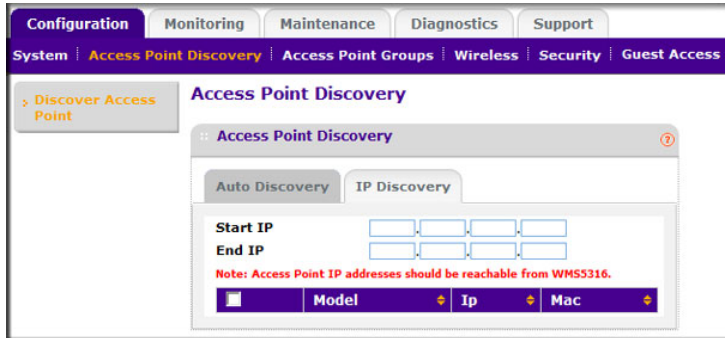
2. Click **Search**.
 - The Wireless Management Software searches for NETGEAR products on the LAN based on MAC address, and identifies which are access points.
 - The access points located through discovery are displayed on the screen.
3. Check the discovery results to make sure that all the access points are listed. See *“Discovery Results”* on page 11.
4. Add the access points as described in *“Adding Access Points”* on page 12.

IP Discovery

Use IP discovery to discover access points in a different IP network than the Wireless Management Software. You can search for a maximum of 255 IP addresses at a time. NETGEAR recommends that you split up your search if you have access points in multiple networks.

To use IP Discovery:

1. On the Configuration tab, select Access Point Discovery, and then click the IP Discovery tab:



2. To specify the range of IP addresses, fill in the **Start IP** and **End IP** fields.
3. Click Search.
 - The Wireless Management Software locates devices on the LAN within the range of IP addresses that you specified.
 - The devices are displayed in a list.
4. Check the discovery results to make sure that all the access points are listed. See *“Discovery Results”* on page 11.
5. Add the access points as described in *“Adding Access Points”* on page 12.

Discovery Results

The effectiveness of the discovery feature depends in part on how the access points on your LAN are set up. If each access point is configured with a unique IP address and is running current firmware, then discovery is usually simple.

If the discovery results are not what you expect, check the following:

- Access points already managed by the Wireless Management Software will not be shown in the discovery list.
- If two or more access points still have their factory default settings, their IP addresses might be identical. If this is the case, the Wireless Management Software discovers one of these access points. Add that access point, change its IP address, and then use discovery to find the next access point.
- If discovery results show unknown access points, it could be due to these reasons:
 - The access point is running an older version of firmware. Upgrade firmware as needed so that discovery can locate the access point.
 - The Wireless Management Software located a NETGEAR access point that is not supported or located a NETGEAR device that is not an access point.

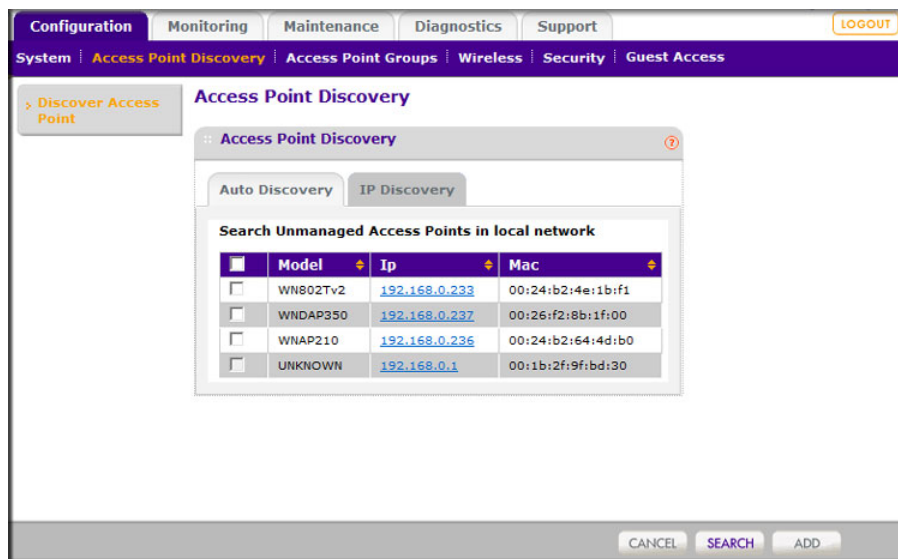
For a list of compatible access point models and their supported firmware, see "[Access Point Supported Firmware Versions](#)" in Appendix A.

- If a new NETGEAR access point is not discovered, it might have a MAC address that the Wireless Management Software does not recognize, though this is not common. See "[Using Discovery OUI](#)" on page 36.

Adding Access Points

After the Wireless Management Software discovers the access points, add them so they can be managed by the Wireless Management Software.

1. On the Access Point Discovery page, select the access point and click **Add**.



2. Enter a password for the access point.

Password

Enter access point password

Password

If the password field is blank, the default password will be used to login to all APs.

Wireless Configuration

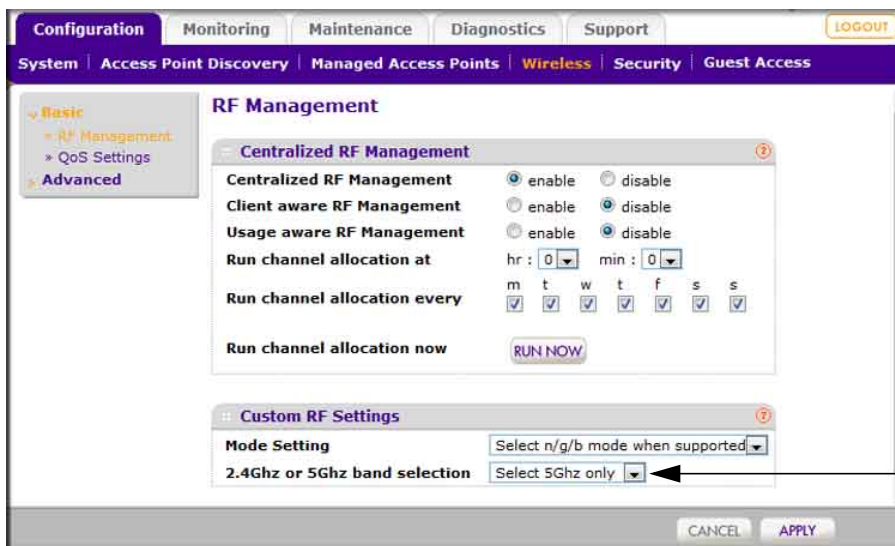
3

You can configure centralized RF management and specify wireless settings in the Basic RF Management page. If you use access point groups, you can use the Advanced Wireless Settings page to customize wireless settings for each group.

Configuring Centralized RF Management

In this screen you can specify RF Management settings. RF Management, when run, optimizes the channel allocation for access points based on clients, user data traffic, and observed nearby RF environment of access points.

1. On the Configuration tab, select Wireless:



This field applies only to model WNDAP330.

2. Specify the Centralized RF Management:
 - **Centralized RF Management:** Selected by default, this **Enable** radio button allows the Wireless Management Software to allocate access point channels based on the access point performance in the local environment. For example, if an access point

experiences interference on a channel, the Wireless Management Software allocates a different channel to that access point.

- **Client aware RF Management:** If this **Enable** radio button is selected, the Wireless Management Software will not modify the channel for an access point with associated clients that would be impacted by the channel change. The Wireless Management Software will wait for the next scheduled channel allocation to adjust the channel.
 - **Usage-aware RF Management:** If this **Enable** radio button is selected, the Wireless Management Software will not modify the channel for an access point that is switching more than 1Mbps of wireless data traffic.
 - **Run Channel Allocation at:** Specify at what time of the day the channel allocation can modify access point RF configuration.
 - **Run Channel Allocation every:** Specify weekly schedule for running channel allocation.
 - **Run Channel Allocation now:** Press button to run channel allocation immediately.
3. Enter the Custom RF Settings:
- **Mode Settings:** Specify the radio mode preference to set on the access points.

Most access points are configured with the fastest mode by default. You can use the **Mode Settings** field to change this. For example, you could specify that an access point that supports wireless-n mode run in b/g mode in order to support clients that do not support wireless n technology.

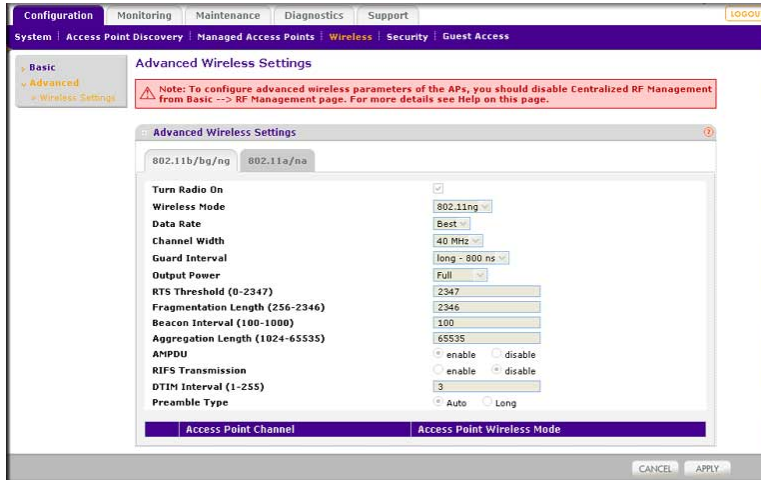
- **2.4GHz or 5GHz band selection:** This selection affects only dual band access points that can only be set to one band at a time such as the WNDAP330. You can use this field to specify which band the access point should use.

Note: For dual concurrent access points, both radio modes are enabled by default.

4. Click **Apply** so that your changes take effect.

Advanced Wireless Settings

This page is for advanced users who wish to control the WLAN settings of the access points manually. On the Configuration tab, select Wireless > Advanced.



To manually specify the WLAN parameters for access points:

1. Disable the Central RF Management feature from the Basic > RF Management page.
This prevents the Wireless Management Software from automatically using RF management and adjusting power and channel settings for the access point group.
2. Specify the settings in the Advanced Wireless Settings screen (see [Table 1](#)).
3. Click **Apply** so that your changes take effect.

Table 1. Advanced Wireless Settings

Field or Setting	Description
Turn Radio On	Disable this option to disable wireless access for the selected mode. To disable all wireless access through this access point, you must turn off the 802.11b/g/n, as well as the 802.11a/n radios.
Wireless Mode	Specify the wireless mode for the access points. Access points use the mode enabled for the group, unless the access point does not support the group setting. In that case, the access point uses the mode providing highest performance. <ul style="list-style-type: none"> • The default setting is 802.11ng mode. • If you specify 802.11b or 802.11bg mode, both 802.11n- and 802.11g-compliant devices can be used with this access point. However, 802.11b devices will not be able to connect. • If you select this option and other settings on this screen are disabled, then you must select the Turn Radio On radio button to enable available options on this screen.
Data Rate	Select the available transmit data rates of the wireless network.

Table 1. Advanced Wireless Settings (Continued)

Field or Setting	Description
Channel Width (11n only)	Select the available channel width of the access point. A wider channel improves the performance, but some legacy devices can only operate on either 20 MHz or 40 MHz.
Guard Interval (11n only)	Select the value that protects transmissions from interference. A shorter guard interval improves performance, but some legacy devices can only operate with a long guard interval.
Output Power	Select the available transmit power of the access point. This option sets the transmit signal strength of the access point. Increasing the power improves performance, but if two or more access points are operating in the same area, on the same channel, it can cause interference.
RTS Threshold (0-2347)	The transmission mechanism (CSMA/CA or CSMA/CD) for the packets. If the packet size is equal to or less than this threshold, the data frame is transmitted immediately. However, if the packet size is larger than the specified value, the transmitting station must send out a Request to Send Threshold (RTS) packet to the receiving station, and must wait for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.
Fragmentation Length (256-2346)	The maximum packet size used for fragmentation of data packets. Packets larger than the specified fragmentation length are broken into smaller packets before being transmitted. The fragmentation length must be an even number.
Beacon Interval (100-1000)	The interval time for each beacon transmission that allows the access point to synchronize the wireless network.
Aggregation Length (1024-65535, 11n only)	The length that defines the maximum length of Aggregated MAC Protocol Data Unit (AMPDU) packets. Larger aggregation lengths might sometimes lead to better network performance. Aggregation is a mechanism used to achieve higher throughput.
AMPDU (11n only)	Allow the aggregation of several MAC frames into a single large frame to achieve higher throughput. Enabling AMPDU might sometimes lead to better network performance.
RIFS Transmission (11n only)	Enable Reduced Interframe Space (RIFS) option to allow transmission of successive frames at different transmit powers. Enabling RIFS might lead to better network performance.
DTIM Interval (1 and 255)	Enter the desired DTIM or the data beacon rate. This indicates the beacon delivery traffic indication message period in multiples of beacon intervals.
Preamble Type (11b/bg only)	A long transmit preamble might provide a more reliable connection or a slightly longer range. A short transmit preamble gives better performance. The Auto settings automatically handles both long and short preambles. The default is Auto.

Configuring QoS

You can use QoS to enable WMM for both upstream traffic from the station to the access point and downstream traffic from the access point to the client station. You can use Basic QoS settings for access points or Advanced QoS Settings for access point groups. These settings are applied only to NETGEAR ProSafe access points that support QoS.

WMM defines the following four queues in decreasing order of priority:

- **Voice:** The highest priority queue with minimum delay, which makes it ideal for applications like VOIP and streaming media.
- **Video:** The second highest priority queue with low delay is given to this queue. Video applications are routed to this queue.
- **Best Effort:** The medium priority queue with medium delay is given to this queue. Most standard IP applications will use this queue.
- **Background:** Low priority queue with high throughput. Applications, such as FTP, which are not time-sensitive but require high throughput can use this queue.

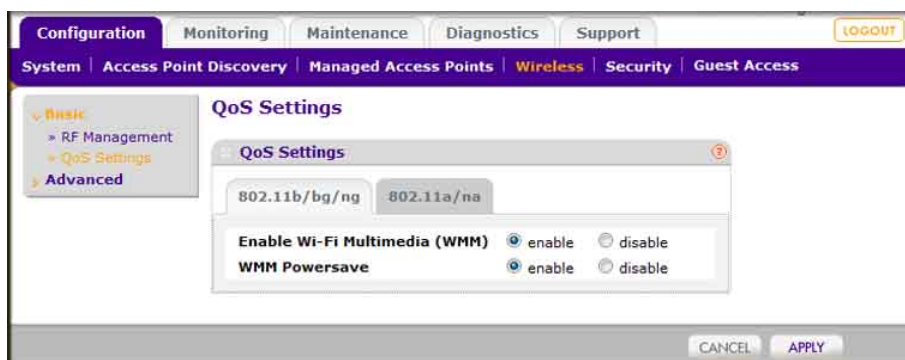
With WMM enabled, QoS prioritizes and coordinates wireless medium access. QoS settings on the access point control downstream traffic to client station (AP EDCA parameters) and the upstream traffic from the station to the access point (station EDCA parameters).

Disabling WMM deactivates QoS control of station EDCA parameters on upstream traffic flowing from the station to the access point. With WMM disabled, you can still set some parameters on the downstream traffic from the access point to the client station (AP EDCA parameters).

QoS for Managed Access Points

To specify QoS settings:

1. On the Configuration tab select Wireless > Basic > QoS Settings:



2. Select either the 802.11b/bg/ng or 802.11a/na tab.
3. Select the **Enable Wi-Fi MultiMedia (WMM)** and **WMM Powersave** options.
4. Click **Apply**.

Security Configuration

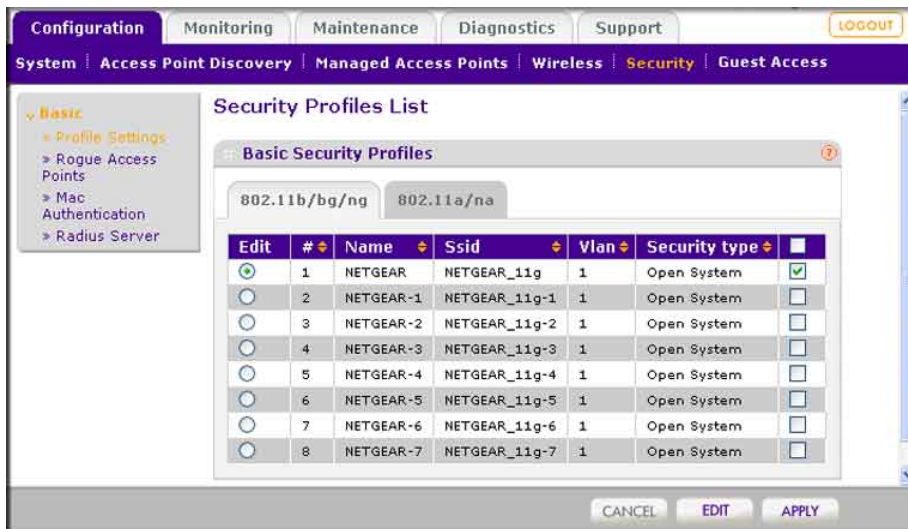
4

Security Profiles List

Details of each wireless network are contained in a security profile. This page lets you edit up to eight Security Profiles per managed access point, depending on the number of profiles each access point supports. Separate profiles are applied to 802.11 b/bg/ng and 802.11 a/na mode radios.

To view or change security profiles:

1. On the Configuration tab, select Security > Basic > Profile Settings.



2. Each Security Profile specifies:
 - **Name:** The unique Profile name, up to 31 alphanumeric characters.
 - **SSID:** The SSID associated with this profile.
 - **VLAN:** The VLAN ID associated with this security profile.
 - **Security:** The security standard, such as WPA-PSK, associated with the profile.

3. Select the **Enable** checkbox to enable (or disable) the corresponding profile.
4. To change the settings of a security profile, select the profile and click the **Edit** button.

Editing a Security Profile

This lets you change the Security Profile settings of the profile that you selected on the Profile Settings page.

The screenshot shows the 'Edit Security Profile' page in the ProSafe 5 AP Wireless Management Software. The page has a navigation bar at the top with tabs for Configuration, Monitoring, Maintenance, Diagnostics, and Support. Below the navigation bar, there are sub-tabs for System, Access Point Discovery, Managed Access Points, Wireless, Security, and Guest Access. The main content area is titled 'Edit Security Profile' and is divided into two sections: 'Profile Definition' and 'Authentication Settings'. The 'Profile Definition' section includes fields for Name (NETGEAR), Wireless Network Name (SSID) (NETGEAR_11g), and Broadcast Wireless Network Name (SSID) (Yes). The 'Authentication Settings' section includes dropdown menus for Network Authentication (Open System), Data Encryption (None), and Wireless Client Security Separation (Disable), along with a text input for VLAN (1).

- **Name:** A unique name for the Security Profile, up to 32 alphanumeric characters. Use meaningful names instead of the default names. The default profile names are Profile1, Profile2, and so on.
- **Wireless Network Name (SSID):** The name of the wireless network associated with this profile.
- **Broadcast Wireless Network Name (SSID):** Enabled by default. If set to **Yes**, the SSID is broadcast. If you disable broadcast of the SSID, only devices that have the correct SSID can connect to the access point.
- **Network Authentication:** The authentication type to be used. See [Table 2 on page 20](#).
- **Data Encryption:** The data encryption type to be used. The options available for data encryption depend on the Network Authentication settings. See [Table 2 on page 20](#).
- **Wireless Client Security Separation:** If enabled, the associated wireless clients will not be able to communicate with each other. This feature is intended for hot spots and other public access situations.
- **VLAN:** The default VLAN ID to be associated with this security profile. This must match the VLAN ID used by other network devices.

The following table shows the data encryption options based on network authentication.

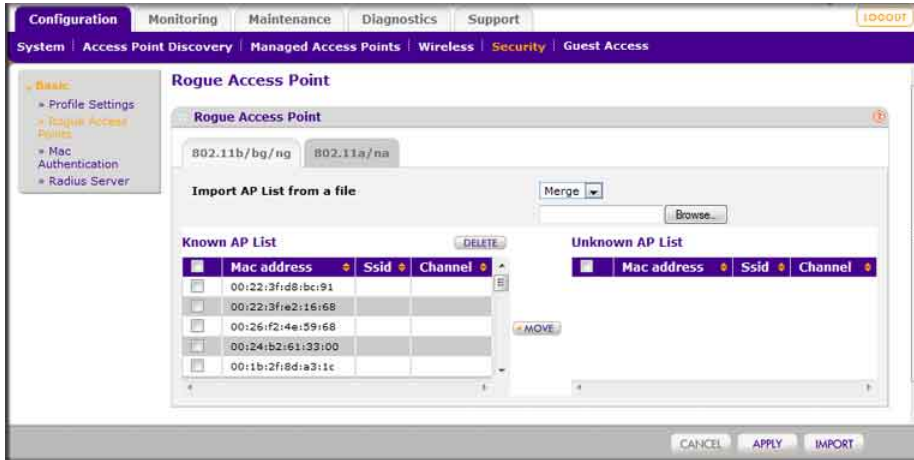
Table 2. Network Authentication and Data Encryption

Network Authentication	Data Encryption	Description
Open	None WEP	No encryption.
Shared Key	WEP	<ul style="list-style-type: none"> 64-bit WEP encryption uses 40/64 bit encryption. 128-bit WEP encryption uses 104/128 bit encryption. 152-bit WEP is a proprietary mode that will only work with other wireless devices that support this mode.
Legacy 802.1x WPA with RADIUS WPA2 with RADIUS	<ul style="list-style-type: none"> Select the WPA2 option only if all clients support WPA2. If selected, you must use AES. WPA/WPA2 with RADIUS allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption. 	All require RADIUS configurations.
WPA-PSK WPA2-PSK	TKIP or TKIP +AES and a WPA passphrase (network key)	Standard encryption method for WPA2.
WPA2-PSK	AES and TKIP + AES	Some clients might support AES with WPA, but this is not supported by this access point.
WPA and WPA2	TKIP + AES encryption and enter the WPA passphrase (network key).	Clients can use either WPA (with TKIP) or WPA2 (with AES).
WPA-PSK/WPA2-PSK	TKIP + AE	Broadcast packets use TKIP. For unicast (point-to-point) transmissions, and WPA clients use TKIP, and WPA2 clients use AES.

Rogue Access Points

Unidentified access points that use the SSID of a legitimate network can present a serious security threat. Rogue Access Point Detection is enabled by default on managed access points. To detect rogue access points, the Wireless Management Software or access point scans the wireless environment on all available channels, looking for unidentified access points.

1. On the Configuration tab select Security > Basic > Rogue Access Points:



The Wireless Management Software can support up to 512 total rogue access points from the Known and Unknown lists combined.

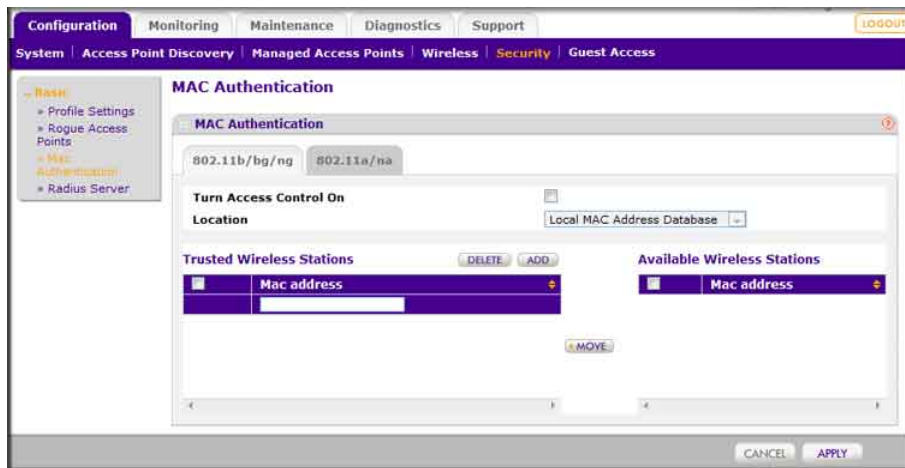
2. Enter the following information:
 - **Import AP List from a file.** This field allows you to import a list of approved access points from a saved file. This file must be a simple text file with one MAC address per line.
 - **Merge.** The current list is maintained and the access points in the imported list is added to the approved list and the Known AP List.
 - **Known AP List.** Approved access points. To remove an access point from this list, select its checkbox and click **Delete**.
 - **Unknown AP List.** Detected unidentified access points.
3. Adjust the Known AP List.
 - You can click **Refresh** to scan for other access points in the vicinity whose details are not in the Known AP List. If such access points are found, they are added to this list.
 - To move an access point from the Unknown AP list to the Known AP list, select its checkbox and click **Move**.
4. When you are finished making changes, click **Apply**.

MAC Authentication

This lets you block the network access privilege of the specified stations with the Wireless Management Software-managed access point. The settings are applied only to managed NETGEAR ProSafe access points.

To set up MAC Authentication:

1. On the Configuration tab, select Security > Basic > MAC Authentication:



A maximum of 512 MAC addresses can be supported.

2. Select the **Apply to all groups** checkbox to apply the settings to all managed access points regardless of group.
3. Select the **Turn Access Control On** checkbox if you want the access point to interact only with stations present in the Trusted Wireless Stations table. This provides an additional layer of security.
4. Select one of the following databases:
 - **Local MAC Address Database:** The access point uses the local MAC address table for access control.
 - **Remote MAC Address Database:** The access point uses the MAC address table on an external Radius server on the LAN for access control.
5. Make sure the correct wireless stations are in the Trusted Wireless Stations list. If you are using access control, only these stations are allowed access to the network through this access point.
 - To remove a wireless station from this table, click **Delete**.
 - To add a wireless station to this table, enter a MAC address and click **Add**.
 - To move a wireless station from the Available Wireless Stations list to the Trusted Wireless Stations list, select it, and click **Move**.
6. Click **Apply** so that your changes take effect.

Radius Server Settings

If you are using a Radius server in your network for authentication, you must configure Radius settings. You can configure four types of servers:

- **Primary Authentication Server:** The main Radius server used for authentication.
- **Secondary Authentication Server:** A Secondary Authentication Server can be configured for use if the Primary Authentication Server fails or is unreachable.
- **Primary Accounting Server:** This server is used for accounting on the network.
- **Secondary Accounting Server:** A Secondary Accounting Server can be configured to use if the Primary Authentication Server fails or is unreachable.

To configure Radius Server Settings:

1. Click the Configuration tab and select Security > Basic > Radius Server Settings:

The screenshot shows the 'Radius Server Settings' configuration page. The page has a navigation bar with tabs for Configuration, Monitoring, Maintenance, Diagnostics, and Support. Below the navigation bar, there are links for System, Access Point Discovery, Managed Access Points, Wireless, Security, and Guest Access. The main content area is titled 'Radius Server Settings' and contains a table with four rows for configuring servers. Below the table is an 'Authentication Settings' section with two input fields and a checkbox.

Radius Server Settings	IP Address	Port	Shared Secret
Primary Authentication Server		1812	*****
Secondary Authentication Server		1812	*****
Primary Accounting Server		1813	*****
Secondary Accounting Server		1813	*****

Authentication Settings

Reauthentication Time (Seconds)

Update Global Key Every (Seconds)

CANCEL APPLY

The primary server is used by default. If it fails, the secondary server is used, if configured.

2. Fill in the **IP Address**, **Port**, and **Shared Secret** fields for each Radius server.
 - The IP Address, Port, and Shared Secret information is required to communicate with the Radius server.
 - The Shared Secret is shared between the wireless access point and the Radius server while authenticating the wireless client.
3. Enter the Authentication Settings.
 - **Re-authentication Time (Seconds):** This is the time interval in seconds after which the supplicant will be authenticated again with the RADIUS server. The default interval is 3600 seconds.
 - **Update Global Key Every (Seconds):** Enable this option to have the Global Key changed according to the time interval specified. If enabled, enter the desired time interval. The default is enable, and the default interval is 1800 Seconds.
4. Click **Apply** so that your changes take effect.

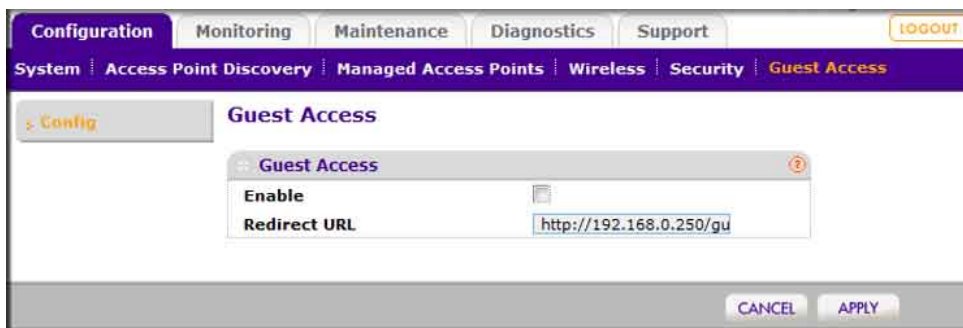
Configuring Guest Access

Guest access settings are useful when you are configuring a public access point. The guest access feature is not a captive portal. You can use guest access to:

- Redirect the user to a guest portal that you specify.
- Allow users to see a splash screen from the wi-fi provider or ask users to enter simple information such as an email address.

To set up guest access:

1. On the Configuration tab, select Guest Access > Config:



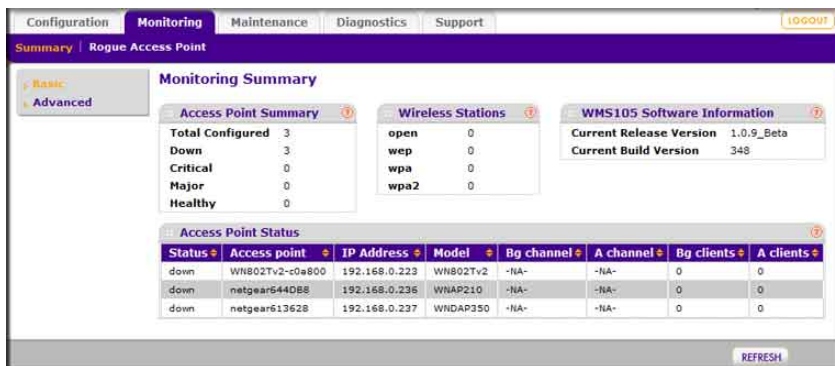
2. Specify the following settings:
 - **Enable:** Enable this if you want all HTTP (TCP, port 80) requests to be routed to the URL you specify in the next field.
 - **Redirect URL:** Enter the URL of the Web server that you want all HTTP requests to be redirected to.
3. Click **Apply** so that your changes take effect.

Monitoring

5

Summary

The Monitoring Summary screen displays a read-only summary of the current managed access point status, rogue access points detected, current wireless stations connected, Wireless Management Software system Information and network usage. Clicking on the individual windows will lead to a new screen showing greater detail.



Access Point Summary

This section displays the status of managed access points.

- **Total Configured:** Total number of managed access points.
- **Down:** Number of managed access points that cannot be pinged.
- **Critical:** The Wireless Management Software can ping these managed access points, but either cannot log in or has detected that the device is different from the one that was configured.
- **Major:** Number of managed access points whose configuration differs from the one set on the Wireless Management Software. This is most likely due to an access point running old firmware or because the Wireless Management Software did configuration changes when the access point was down or offline.
- **Healthy:** Managed access points running properly.

Wireless Stations

This section displays the count of the wireless stations currently associated with managed access points.

- **open:** Wireless stations connected to managed access points using security profiles configured with open mode.
- **wep:** Wireless stations connected to managed access points using security profiles configured with WEP.
- **wpa:** Wireless stations connected to managed access points using security profiles configured with WPA security.
- **wpa2:** Wireless stations connected to managed access points using security profiles configured with WPA2 security.

Access Point Status

On the Monitoring tab select Summary > Advanced > Access Point Status:



Status	Group	Access point	Ip address	Model	Bg channel	A channel	Bg clients	A clients
healthy	basic	netgear4E18F1	192.168.0.233	WN802Tv2	11	-NA-	0	0
healthy	basic	netgear8B1F08	192.168.0.237	WNDAP350	11	157	0	0
healthy	basic	netgear644D88	192.168.0.236	WNAP210	5	-NA-	0	0

The access point status screen displays a read-only status summary of managed access points. Each access point entry specifies:

- **Status:** Access point connection and configuration status.
- **Access Point:** Netbios name of the access point.
- **IP address:** Management IP address used by the Wireless Management Software to connect to the access point.
- **Model:** The access point model.
- **B/G channel:** The b/g/n mode channel configured on the access point
- **A channel:** The a/n mode channel configured for the access point.
- **B/G clients:** The number of client stations connected to the access point using the 2.4GHz channel
- **A clients:** The number of client stations connected to the access point using the 5GHz channel.

Click **Refresh** to update the displayed status of access points. Click **Details** to display detailed status of specific managed access points.

Access Point Status Details

From the Access Point Status screen, click the **Details** button to view this page.

You can use the **Refresh** button to update statistics and information.

The Access Point Status screen shows configuration settings, current wireless settings, current clients and current traffic statistics.

- **Access Point Name:** The access point's NetBIOS name.
- **Model:** The managed access point's model.
- **Group:** The configured group of managed access point.
- **IP Address:** The IP Address of managed access point.
- **Ethernet MAC Address:** The Ethernet MAC address of managed access point.
- **2.4 GHz Channel:** 2.4 GHz channel configured on access point; set to -NA- if not available.
- **5 GHz Channel:** 5 GHz channel configured on access point; set to -NA- if not available.
- **Load Balancing:** Load balancing enable/disable status for access point.

The screenshot shows the 'Access Point Status' window with the following sections:

- Access Point Details:**
 - Access Point: netgear4E1BF1
 - Model: WN802Tv2
 - Group: basic
 - IP Address: 192.168.0.233
 - Ethernet MAC Address: 00:24:b2:4e:1b:f1
 - 2.4 GHz Channel: 11
 - 5 GHz Channel: -NA-
 - Channel Management: Centralized
 - Load Balancing: Disabled
- ProfileInfo:**

Type	Ssid	Security	Vlan
802.11b/bg/ng	NETGEAR_11g	open	1
- Client Info:**

Mac	Ssid	Channel	Mode	Auth	Cipher
No clients listed.					
- Rogue Access Points(802.11b/bg/ng):**
 - Rogue Access Points reported: 0
 - Rogue Access Points in same channel: 0
 - Rogue Access Points in interfering channel: 0

Buttons: REFRESH, CLOSE

Profile Information

The section displays configured and enabled security profiles on the access point.

- **Type:** 802.11 b/bg/ng or 802.11 a/na mode for security profile.
- **SSID:** Wireless Network SSID.
- **Security:** The mode of security configured for the profile.
- **VLAN:** VLAN configured for the security profile.

Client Information

This section displays access point client station information.

- **MAC:** Wireless MAC of the access point client.
- **SSID:** Wireless SSID configured on the managed access point to which the client connects.
- **Channel:** The channel which client is using to connect.
- **Mode:** The mode (802.11 b/bg/ng or 802.11 a/na) for the security profile.
- **Auth:** The authentication mode (open, WEP, WPA, or WPA2) of security.

Rogue Access Points

This section displays rogue or neighboring access points detected by the managed access point.

- Rogue Access Points Reported.
- Rogue Access Points in same channel.
- Rogue Access Points in interfering channels.

Client Status

On the Monitoring tab select Summary > Advanced > Client Status:



The Client Status list specifies detailed information about each client node currently associated with managed access points.

- Use the **Refresh** button to update the list of available wireless stations.
- Use the **Details** button to get details of a selected wireless station.

Monitoring Rogue Access Points

On the Monitoring tab you can view rogue or unknown access points.

To display unknown access points, select Rogue Access Point > Unknown:

Mac address	Ssid	Channel	Privacy	Rate	Beacon int.	# of beacons	Last beacon	Neighbour access points
00:0fccc6:1f:6c	7141 0240	6	1	54.00	100	1	Sun Mar 29 17:52:52 2009	netgearBE1F08
00:124b2:4e:1b:f1	103_bast	11	0	270.00	100	2332	Sun Mar 29 18:06:41 2009	netgearBE1F08
00:e0:02:12:35:88	NETGEAR	11	0	130.00	100	1099	Sun Mar 29 18:06:41 2009	netgearBE1F08
00:126:f2:bb:7e:58	3500I	11	1	144.44	100	676	Sun Mar 29 18:06:36 2009	netgearBE1F08
00:126:f2:9a:0d:00	NETGEAR_11g	11	0	130.00	100	404	Sun Mar 29 18:06:12 2009	netgearBE1F08
00:126:f2:9a:24:20	NETGEAR_11g	11	0	130.00	100	328	Sun Mar 29 18:06:29 2009	netgearBE1F08
00:1f:33:7a:ea:2c	NETGEAR	11	0	130.00	100	1419	Sun Mar 29 18:06:41 2009	netgearBE1F08
00:124:b0:3f:79:bb	NETGEAR	11	0	130.00	400	423	Sun Mar 29 18:06:30 2009	netgearBE1F08
00:1f:33:7a:ea:88	NETGEAR	11	0	130.00	100	340	Sun Mar 29 18:06:39 2009	netgearBE1F08
00:126:f2:9a:12:80	NETGEAR_11g	11	0	130.00	100	104	Sun Mar 29 18:06:12 2009	netgearBE1F08

You can click **Refresh** to update the access point list or click **Export** to save the list to a file.

To display the list of known rogue access points, on the Monitoring tab select Rogue Access Point > Known:.



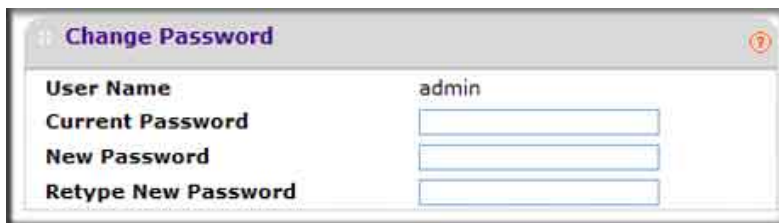
You can click **Refresh** to update the access point list or click **Export** to save the list to a file.

Changing Passwords

This page lets you to change the access point administrator's password.

Note: If you changed the password and do not remember what it is, reinstall the Wireless Management System software.

From the Maintenance tab select Password:



Change Password	
User Name	admin
Current Password	<input type="text"/>
New Password	<input type="text"/>
Retype New Password	<input type="text"/>

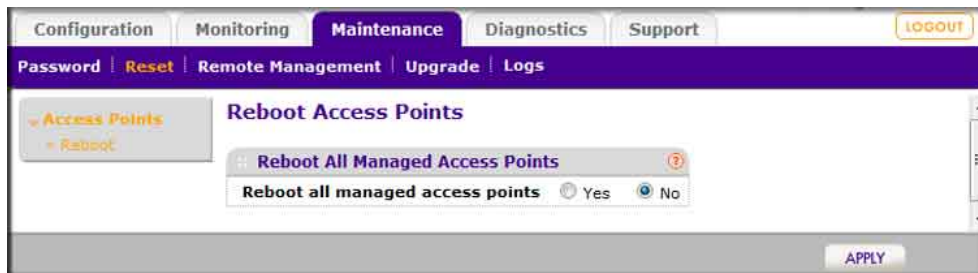
To change the password:

1. Type the old password. (The default password for the user name admin is **password**)
2. Type a new password, then type it again in the **Repeat New Password** field to confirm it.
3. Be sure to record it in a secure location.
4. Click **Apply** so that your changes take effect or click **Cancel** to keep the current password.

Reset

The Reset screen lets you reboot managed access points.

1. On the Maintenance tab select Reset > Access Points > Reboot:



2. Select the **Yes** radio button.
3. Click **Apply** to reboot the access points.

SNMP

You can use SNMP for the Wireless Management Software. Enable SNMP to allow the SNMP network management software, such as HP OpenView, to monitor the Wireless Management Software by using SNMPv1/v2 protocol.

On the Maintenance tab, select Remote Management > System > SNMP:



- **SNMP** checkbox: Enable SNMP for the Wireless Management Software.
- **Read-Only Community Name:** The community string to allow the SNMP manager to read the WMS105 MIB objects.
- **Read-Write Community Name:** The community string to allow the SNMP manager to read and write the WMS105 MIB objects.
- **Trap Community Name:** The community name which is associated with the IP address to Receive Traps.
- **IP address to Receive Traps:** The IP address of the SNMP manager to receive traps sent from the Wireless Management Software.

- **Trap Port:** The default port on which SNMP manager receives traps sent from the Wireless Management Software is 162.
- **SNMP Manager IP:** Restrict access to specified SNMP manager for doing SNMP v1/v2. Set this as 255.255.255.255 to allow any SNMP manager to access.

When you are finished making changes, click **Apply** to save your settings.

Remote Management

You can enable SSH or Telnet to remotely log in to the controller. From the Maintenance tab select Remote Management > System > Remote Console:



1. Select the radio button for SSH or Telnet:
 - **Secure Shell (SSH):** If set to **Enable**, the Wireless Management Software allows remote access by using Secure Shell.
 - **Telnet:** If set to **Enable**, the Wireless Management Software allows remote access by using Telnet.
2. Click **Apply** to save your settings.

Upgrading Access Point Firmware

You can install a new firmware for the access points using the Access Point Upgrade page.



WARNING!

In some cases, such as a major upgrade, you might need to erase the configuration of your access point after upgrading it.

See the Release Notes included with the software to find out if you need to reconfigure the access point. Reconfiguring access points already managed by the Wireless Management Software requires only the IP address to be set manually. The Wireless Management Software restores configuration for already managed access points running supported software version.

To upgrade the access point software:

1. Go to the NETGEAR web site at www.NETGEAR.com customer service downloads section to get new versions of the access point software for supported models. After downloading an upgrade file, you might need to unzip (uncompress) it before upgrading the access point.



WARNING!

Once you click Upload do NOT interrupt the process of sending the software to the access point and restarting the access point.

2. Download the new software for a specific access point model to upgrade.
3. If not done automatically, uncompress the downloaded file. If included, read the Release Notes before continuing.
4. On the Maintenance tab select Upgrade > Access Point Upgrade:

5. Make sure that status of the managed access point to be upgraded is healthy. Select the managed access point model from the drop-down list; only models of managed access points are in this list.
6. Click **Browse**.
7. Locate and select the file you just downloaded.
8. Click **Upload** to send the software to the access point.

This loads the new software into the access point and causes the access point to restart.



WARNING!

Do not try to go online, turn off the access point, shut down the computer or the Wireless Management Software or do anything else to the access point or the Wireless Management Software until the access point finishes restarting! When the Test light turns off, wait a few more seconds before doing anything.

9. Check the firmware version on the Upgrade page to verify that your access point now has the new software installed.

Backing up Configuration Settings

Once you have the Wireless Management Software working properly, you should back up the information to have it available if something goes wrong. When you back up the settings, they are saved as a file on your computer.

To back up the Wireless Management Software settings:

1. On the Maintenance tab select Upgrade > Backup:



2. Click the **Backup** button to create a backup file of the current settings:
3. If you do not have your browser set up to save downloaded files automatically, then find a location where you want to save the file, and rename it if you like.

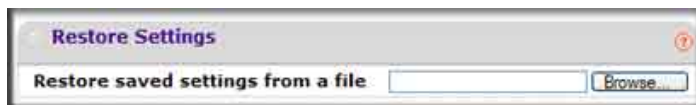
If your browser is set up to save downloaded files automatically, the file is saved to your browser's download location on the hard disk

4. Click **Backup**.

Restoring Settings from a File

To restore settings from a backup file:

1. On the Maintenance tab select Upgrade > Restore Settings:



2. Click **Browse**.
3. Locate and select the previously saved backup file, then click **Apply**.

After restoring previous settings, the Wireless Management Software restarts. This takes about one minute.



WARNING!

Do not try to go online, turn off the Wireless Management Software, shut down the computer or do anything else until it finishes restarting! When the Test light turns off, wait a few more seconds before doing anything with the Wireless Management Software.

Downloading Wireless Management Software Logs

Maintenance logs allow backup of the logs collected on the Wireless Management Software. In the event of a problem or failure, these logs along with backed up configuration settings help developers determine the cause.



To download logs:

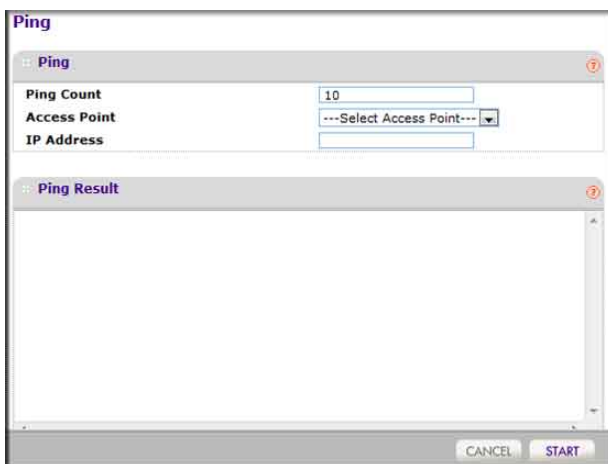
1. On the Maintenance Tab, select Logs.
2. Click **Backup** to create a backup file of the current logs.
3. If you do not have your browser set up to save downloaded files automatically, then locate where you want to save the file, rename it if you like.

If your browser is set up to save downloaded files automatically, the file will be saved to your browser's download location on the hard disk

4. Click **Backup**.

Diagnostic Ping Window

This window provides a way to verify ping connectivity from the Wireless Management Software to a managed access point. A managed access point can be selected from the **Access Point** drop-down list. The IP address of the access point to be pinged is displayed in the **IP Address** field.



1. Specify the number of pings to be tried in the **Ping Count** field.
2. Click **Start** to begin pinging the selected access point.
3. When you are finished, click **Cancel** to stop the pinging.

Using Discovery OUI

The Wireless Management Software discovers NETGEAR access points on the LAN from the OUI (Organizationally Unique Identifier) of their unique MAC addresses. The first half of the MAC address is the OUI. Usually, this happens without incident during discovery. OUIs are allocated to businesses that produce products with MAC addresses.

Discovery OUI is not often needed, but is useful in the following circumstances:

- There is a new NETGEAR access point that has a new OUI.
- The WMS105 controller is running older firmware that does not recognize the new OUI.
- You do not want to update the WMS105 firmware.

You can use Discovery OUI to register and discover the access point. Click the System tab and select Advanced > Discovery OUI:



To change the settings:

1. Click **Add** to add a OUI to the list or click **Delete** to remove it.

Note: OUIs already allocated for NETGEAR devices are preconfigured and cannot be deleted

2. Click the **Apply** button to save your changes.

Access Point Compatibility



Access Point Supported Firmware Versions

Access Point Model	Supported Firmware	Security Profiles per Radio	Auto Channel
WNDAP330	WNDAP330_V3.0.4	8	Yes
WNDAP350	WNDAP350_V2.0	8	Yes
WNAP210	WNAP210_2.0.8	8	Yes
WG302v2	5.2.3	8	Yes
WG103	WG103_2.0	8	No
WN802Tv2	WN802Tv2_V3.1.2	1	Limited to channel distribution without neighbor map
WG602v4	V1.1.0	1	Limited to channel distribution without neighbor map

For the latest firmware images, visit the NETGEAR support web site:
<http://www.netgear.com/support>.

Software Features and Access Point Compatibility

Access Point Model	Topology	VLAN Config	Rogue Access Points	Remote Access SSH Telnet	Guest Access	Client Separation	Syslog	NTP (Time Server)
WNDAP330	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
WNDAP350	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WNAP210	Yes	Yes	Yes	Yes	Yes	Yes	SNS	Yes
WG302v2	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
WG103	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WN802Tv2	No	No	No	No	No	Yes	Yes	Yes
WG602v4	No	No	No	No	No	No	No	No

Index

A

- access point
 - WLAN settings [3-15](#)
- access point discovery [2-9](#)
 - IP discovery [2-10](#)
- access points
 - adding [2-12](#)
 - discovery results [2-11](#)
 - passwords [2-12](#)
 - rogue [4-20](#), [5-26](#)
 - status [5-25](#), [5-26](#), [5-27](#)
 - supported firmware [A-37](#)
- access, guest [4-24](#)
- adding access points [2-12](#)
- authentication, MAC [4-21](#)
- Auto Discovery [2-9](#)

B

- backing up [6-34](#)

C

- centralized RF management [3-13](#)
- clients, status [5-28](#)
- configuration settings
 - backing up [6-34](#)
 - restoring [6-34](#)

D

- diagnostics, Ping [6-35](#)
- discovering access points [2-9](#)
 - Auto Discovery [2-9](#)
 - IP discovery [2-10](#)
 - results [2-11](#)
- Discovery OUI [6-36](#)

F

- firmware
 - access point supported [A-37](#)
 - upgrading [6-32](#)

G

- General settings [1-6](#)
- guest access [4-24](#)

I

- IP discovery [2-10](#)

L

- logging in to the Wireless Management System [1-6](#)
- logs, system [6-35](#)

M

- MAC authentication [4-21](#)
- monitoring
 - access point summary [5-25](#)
 - client status [5-28](#)

O

- OUI discovery [6-36](#)

P

- passwords [1-6](#)
 - changing [6-30](#)
- passwords for access points [2-12](#)
- Ping [6-35](#)

Q

- QoS [3-17](#)
- QoS for managed access points [3-17](#)

R

- Radius server configuration [4-23](#)
- rebooting [6-31](#)
- remote console [6-32](#)
- remote management [6-32](#)
- resetting [6-31](#)
- restoring settings from a file [6-34](#)

RF management, centralized **3-13**
rogue access points **4-20, 5-26**

S

Security Profiles, editing **4-19**

SNMP **6-31**

status

 access point details **5-27**

 access points **5-25, 5-26**

 client **5-28**

 wireless stations **5-26**

Syslog **1-8**

system logs **6-35**

T

time, setting **1-7**

U

upgrading firmware **6-32**

W

wireless

 access points **3-15**

 centralized RF management **3-13**

wireless stations status **5-26**